DIGITAL DIRECTORS NETWORK

Bob Zukis
Chief Executive Officer
310.528.9945
ceo@digitaldirectors.network

May 8, 2022

SEC Commissioners
Securities and Exchange Commission
Washington, D.C. USA

Re: **FILE NUMBER S7-09-22 — COMMENTS ON CYBERSECURITY RISK MANAGEMENT, STRATEGY, GOVERNANCE, AND INCIDENT DISCLOSURE**

Ladies and Gentlemen of the Commission,

We are pleased to provide our comments on the proposed rules referenced in **FILE NUMBER S7-09-22.**

We are a curated network of over 700 U.S. technology executives and corporate directors working exclusively on advancing leading boardroom policies and practices in cyber governance. We are the leader in advancing these issues in America as this was our founding mission when we launched in October of 2017. Our executive network includes CIOs, CISOs, CROs, and corporate directors from some of America's leading public and private companies and boardrooms.

Our opinions reflect the most developed perspective and body of work on cyber governance in America.

PROPOSED AMENDMENT ITEM E: DISCLOSURE REGARDING THE BOARD OF DIRECTORS' CYBERSECURITY EXPERTISE ITEM 407 REGULATION S-K

Together with the 700+ technology leaders who are DDN members we STRONGLY support this amendment and the changes it will introduce with Item 407(j) requiring disclosure of boardroom cyber expertise.

The item E amendment is singularly the **highest impact, lowest effort** proposal being suggested that will materially lower cyber risk exposure for America's public companies. Strengthening America's boardrooms as a critical control point in cybersecurity is an issue of national security. This issue is also core to the competitiveness of American businesses and one squarely in the interest of investors and consumers.

All other proposals in S7-09-22 will be strengthened through this foundational, common-sense, overdue, and easily implementable boardroom reform.

We would like to call the Commissions attention to the following general observations backing up our support for this amendment and our detailed answers to questions 26-37 that follow.

DIGITAL DIRECTORS NETWORK

Bob Zukis
Chief Executive Officer
310.528.9945
ceo@digitaldirectors.network

The SOX Boardroom Financial Expertise Disclosure Precedent

We call the Commission's attention to 2022 being the twentieth anniversary of The Sarbanes Oxley Act (SOX) of 2002. As you know, a similar requirement concerning boardroom disclosure of financial expertise was passed as a part of that legislation. In hindsight, it would be hard to argue against the presence of directors' financial expertise in America's public company corporate boardrooms.

I identified the synergies between SOX and the need for boardroom cyber expertise in an article I wrote for The Conference Board in 2016 titled *Are Cyber Experts On Boards Inevitable?*[1] My conclusion from this article stated:

> *Directors who do not have the ability to ask the right cybersecurity question, will never get the right answer. Cybersecurity governance ground zero starts in the American corporate boardroom with competent cybersecurity directors. Whether forced by regulators, pressured by activists, or added by a board that recognizes that good corporate governance needs cybersecurity competent directors, a decade from now, we'll look back in disbelief at what is today, the novel concept of having cybersecurity skills in the American corporate boardroom.*

In 2012, after a decade of SOX, research from the SEC filings corporate governance database of Big 4 accounting firm EY observed that:

> *In 2003, only a small number of audit committee members were financial experts. Today, almost one-half of all audit committee members are identified through proxy statement disclosure as meeting the definition of a financial expert.*[2]

More narrowly, recruiting firm Spencer Stuart observed that for the companies in the S&P 500:

> *In 2003 21 percent of boards reported having a financial expert -- 146 financial experts in total -- versus 2012, when 100 percent of S&P 500 boards report having at least one financial expert for a total of 1,096.*[3]

The financial expertise disclosure provision in SOX quickly and effectively infused boardroom accountability and competencies that positively and materially impacted the financial reporting

[1] Zukis, Bob. "Are Cyber Experts On Boards Inevitable?" The Conference Board, June 16, 2016 https://www.conference-board.org/blog/postdetail.cfm?post=5917

[2] The Sarbanes-Oxley Act at 10 Enhancing the reliability of financial reporting and audit quality. EY. 2012. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwietL7KuND3AhUxD0QIHQWIAUwQFnoECAYQAQ&url=https%3A%2F%2Fpdf4pro.com%2Fcdn%2Fthe-sarbanes-oxley-act-at-10-ey-united-states-3089d.pdf&usg=AOvVaw3ID8aNNN-XpsdX3Ub5vTfA

[3] UVA Darden Ideas to Action: Marketers on board the secret ingredient for firm growth, University of Virginia Darden School. October 30, 2108. https://ideas.darden.virginia.edu/marketers-on-board-the-secret-ingredient-to-firm-growth

Bob Zukis
Chief Executive Officer
310.528.9945
ceo@digitaldirectors.network

and accounting quality of American companies. In hindsight, it is difficult to believe that it was only twenty years ago when it was a novel concept to have expertise in America's boardrooms that understood a financial statement. The time has now arrived to fix the cyber expertise shortcoming in America's boardrooms.

Corporate directors not only need to ask the right questions on cyber risk, but they also need to understand the answers. While financial and accounting concepts have been taught as a part of core higher education business curriculums for decades, it still took SOX to force boards to introduce the depth of this core competency into the corporate boardroom and governance system. Cybersecurity is not a core competency taught in most university business curriculums which makes it a much larger boardroom competency gap amongst the vast majority of America's current cohort of corporate directors.

Consequently, it must be expressly introduced into America's corporate boardrooms which the proposed rule will efficiently do.

Self-regulatory practices that could have introduced cyber expertise into the boardroom have failed as only a small percentage of America's boardrooms have voluntarily adopted this leading practice. However, boardroom cyber expertise precedent does exist from some of America's leading companies such as FedEx, AIG, GM, Hasbro, Verisign, and some others. This emergent practice is early validation of the recognized need to strengthen this aspect of corporate governance. Holding corporate boards accountable with an easily implementable disclosure standard will positively and materially improve the cyber risk profile of America's public companies. This proposed rule will also create a positive spillover effect on America's private company's boardroom cyber expertise. Something that occurred after SOX as a result of the boardroom financial expertise disclosure rule for public companies.

Without cyber expertise in the boardroom, the vast majority of America's boardrooms are not capable of governing the significant cyber risks threatening and impairing American business. The boardroom is a critical part of every company's overall system of cyber risk management. From setting the cyber tone at the top, to monitoring and advising management teams this competency needs to be a core and effective boardroom competency.

We believe this proposed rule is a necessary, reasonable, and foundational corporate governance step that will quickly improve America's cyber risk management posture.

The precedent of requiring disclosure of financial expertise in America's corporate boardrooms materially improved the boardroom as a critical control in financial reporting. This 2002 corporate governance reform strengthened America's capital markets alongside the financial and accounting management practices and policies of American companies.

This type of boardroom reform has worked before in American corporate governance. It will work again to reduce cyber risk as cyber expertise is brought into America's boardrooms.

DIGITAL DIRECTORS NETWORK

Bob Zukis
Chief Executive Officer
310.528.9945
ceo@digitaldirectors.network

Adding Cyber Expertise in the Boardroom Will Strengthen America's National Security and Economic Growth

Leading technology industry analyst IDC estimates that 65% of global GDP will be digitized in 2022[4]. In 2019 the World Economic Forum also declared that 60% of global GDP would be digitized by 2022, contrasted with the statement that only 45% of people trust that technology will improve their lives[5]. America's investors, consumers, and other corporate stakeholders deserve to know that the corporate boards governing the companies they invest in and do business with are competent to govern cyber risk at the senior-most levels of the organization.

As the most cyber-attacked country in the world, America's corporate governance weakness in cyber risk means America's companies face significantly higher levels of litigation, equity, and financial risk than other companies worldwide. Without this proposed rule, this weakness will remain, all but guaranteeing that cyber-attacks will not only continue but escalate. American companies will remain the preferred target of attackers which will impair economic growth and weaken national security.

The emergence of systemic cyber risk also requires every American public and private company to strengthen their cyber governance, not just a few. Cyber risk that can start in one organization can rapidly move between companies as was experienced with the SolarWinds breach. Attackers are increasingly looking to exploit systemic cyber risk in this manner.

This requires a far-reaching and implementable approach to improving cyber governance for any American company, which we believe your proposed rule offers. Establishing cyber expertise as a leading practice in America's public company boardrooms is a precedent that will spread to private companies.

Effective corporate governance over any issue starts with the competencies of the corporate directors in the boardroom. We strongly urge the SEC to approve this proposed rule to strengthen cyber governance in the boardroom and secure America's path toward the digital future.

Cyber Experts Will Strengthen The Entire Corporate Governance Agenda

There is often a misinformed perception that cyber experts are limited as boardroom contributors due to their technical acumen. A similar argument was made around financial expertise twenty years ago with the financial expertise disclosure requirement proposed with Sarbanes-Oxley.

[4] IDC FutureScape: Worldwide Digital Transformation Predictions 2021. (Framingham. IDC. October 2020). https://www.idc.com/getdoc.jsp?containerId=prUS46967420

[5] Our Shared Digital Future Responsible Digital Transformation – Board Briefing. (Geneva. World Economic Forum. 2019). https://www3.weforum.org/docs/WEF_Responsible_Digital_Transformation.pdf

Bob Zukis
Chief Executive Officer
310.528.9945
ceo@digitaldirectors.network

While this will be true for some cyber experts, as it was for some financial experts, it is not true for all of them. Many cyber experts are well-rounded business executives who also happen to understand how to protect the vast sources of business value being created by today's and tomorrow's information technologies.

Our organization is the only one in the world that has been recruiting, developing, and training America's leading technology executives for boardroom service. Over 700 members strong, many of these executives have also completed the world's leading business school caliber boardroom readiness executive education program which was launched in 2019. Most of these executives are actively pursuing corporate directorship, and already have boardroom experience with their board, or frequently an external board.

These boardroom and cyber experts have executive experience, boardroom experience, and demonstrated deep competencies as digital and cyber experts and would meet the suggested criteria for cyber expertise included in the proposed rule. Moreover, they have also been trained and certified on the DiRECTOR™ framework to understand and govern systemic risk in complex digital business systems. There exists today, a deep pool of boardroom-ready, capable and willing cyber experts able to step into America's corporate boardrooms.

We have included comments to your specific questions below:

Question 26: Would proposed Item 407(j) disclosure provide information that investors would find useful? Should it be modified in any way?

DDN Answer 26: It would be extremely useful for reasonable investors as it is a material disclosure of information critical to their assessment of business, financial, and equity risk as it identifies if the boardroom is a functioning control point in cyber risk management. The disclosure also sends a strong signal to potential attackers and sends a strong internal signal to the entire organization by establishing the cyber tone at the top of the organization.

Question 27: Should we require disclosure of the names of persons with cybersecurity expertise on the board of directors, as currently proposed in Item 407(j)? Would a requirement to name such persons have the unintended effect of deterring persons with this expertise from serving on a board of directors?

DDN Answer 27: Naming an individual is essential to establishing accountability and ensuring boardroom depth of cyber expertise. It will not dissuade true cyber experts from serving on a corporate board, which is also the reason why they should be named. There is a significant difference in cyber expertise between a finance executive who sits on a cybersecurity company's board, and an executive who has been a cyber practitioner with formally acquired and applied competencies in cybersecurity. Absent the requirement to state a name, the former director would likely drive the undesired practice of deeming the rule to have been satisfied. However, the intent of the rule, and the need, is clearly to drive the presence of deep cyber expertise into the

Bob Zukis
Chief Executive Officer
310.528.9945
ceo@digitaldirectors.network

boardroom. The complexity of cyber risk and the rapidly changing nature of it warrants depth of cyber expertise, not casual familiarity with it. Those with an applied cyber background will not be dissuaded. Our 700 plus members are testament to this, they are willing, able, and ready to serve in the boardroom as named cyber experts.

Question 28: When a registrant does not have a person with cybersecurity expertise on its board of directors, should the registrant be stated expressly that this is the case under proposed Item 407(j)? As proposed, we would not require registrant to make such an explicit statement.

DDN Answer 28: Yes, the absence of cyber expertise should be required as an explicit disclosure with the modification of allowing an issuer greater latitude to "comply or explain" as is contemplated in proposed Senate Bill S. 808 – The Cybersecurity Disclosure Bill of 2021.[6] This draft Bill states that:

> (2) if no member of the governing body of the reporting company has expertise or experience in cybersecurity, to describe what other aspects of the reporting company's cybersecurity were taken into account by any person, such as an official serving on a nominating committee, that is responsible for identifying and evaluating nominees for membership to the governing body.

As a core corporate governance principle, "comply or explain" allows issuers the latitude to address boardroom cyber expertise in multiple ways. Expanding the disclosure requirement to allow disclosure of other cybersecurity practices or policies would provide issuers the option to "buy" or "rent" cyber expertise in the boardroom. "Buying" reflects the addition of a director who is a functional cyber expert onto the board. This is a low-cost, high-impact solution that can be adopted in the short term. It will have a material impact on improving corporate governance and reducing cyber risk for the issuer. We are strong advocates for "buying" as building up equity in cyber risk governance will deliver the highest levels of long-term cyber resiliency against the rapidly changing cyber threat landscape.

However, our suggested modification would allow corporate boards the flexibility to disclose how they "rent" cyber expertise from the many individuals or organizations who are immediately capable of providing boardroom and management advice on these issues. Actions that corporate boards can take in the short term, other than adding a director who is a cyber expert to their director ranks, include:

- Annual and regular executive education for the full board on cybersecurity governance and cyber risk.
- Hiring firms or individuals who are third-party cyber experts in a similar model of compensation consultants or external auditors that can advise, assess, and update the board on cyber risk and management's cyber risk practices, policies, and effectiveness.

[6] Reed, Jack, et al. S. 808 Cybersecurity Disclosure Bill of 2021. 117th Congress (2021-2022). https://www.congress.gov/bill/117th-congress/senate-bill/808

Bob Zukis
Chief Executive Officer
310.528.9945
ceo@digitaldirectors.network

Question 29: Proposed Item 407(J) would require registrants to describe fully the nature of a board member's expertise in cybersecurity without mandating specific disclosures. Is there particular information that we should instead require a registrant to disclose with respect to a board member's expertise in cybersecurity?

DDN Answer 29: No, we do not believe that further prescriptive in-depth disclosure of specific attributes of cyber expertise, e.g., job title, degree, is practical or warranted. Furthermore, we believe your suggested criteria exhibiting the applied competency base is adequate as it reflects the deep operational expectation of cyber competencies expected of a boardroom cyber expert. The debate that took place with financial expertise addressed the issue of job titles, which was abandoned in the final regulations and followed the path of allowing issuers the latitude to assess the demonstrated operational aptitude gained through formal education and application. This is the correct approach as it will allow issuers some flexibility, and keep the candidate pool deep, while also allowing issuers to assess the ability of cyber experts more broadly as business experts and their capacity to contribute to the overall corporate governance agenda. It will avoid a "check the box" approach a prescriptive list of criteria may create.

Question 30: As proposed, Item 407(J) includes a non-exclusive list of criteria that a company should consider in determining whether a director has expertise in cybersecurity. Are these factors for registrants to consider useful in determining cybersecurity expertise? Should the list be revised, eliminated, or supplemented?

DDN Answer 30: See DDN Answer 29.

Question 31: Would the Item 407(j) disclosure requirements have the unintended effect of undermining a registrant's cybersecurity defense efforts or otherwise impose undue burdens on registrants? If so, how?

DDN Answer 31: It would not impose an undue burden or cause undue negative consequences, quite the opposite. The proposed rule is lightweight and will strengthen all other proposed cyber rules. Moreover, it will strengthen both the boardroom as a cybersecurity control point in the organization's entire system of cybersecurity AND send powerful signals internally and externally that the senior-most level of the business is cyber competent.

Question 32: Should 407(j) disclosure of board expertise be required in an annual statement and proxy report as proposed?

DDN Answer 31: Yes, as this core cyber control is of interest to all stakeholders, as such, the distribution of the nature of its presence should be as wide as possible in an annual statement and proxy.

Bob Zukis
Chief Executive Officer
310.528.9945
ceo@digitaldirectors.network

Question 33: To what extent would disclosure under proposed Item 407(j) overlap with disclosure required under Item 401(e) of Regulation S-K with respect to the business experience of directors? Are there alternative approaches that would avoid duplicative disclosure without being cumbersome for investors?

DDN Answer 33: We believe it would overlap very little. Cybersecurity expertise is not currently a widely tracked specific corporate director area of expertise on internal or external director competency matrices. We believe in practice Item 407(j) would enhance 401(e) business experience disclosures to identify other corporate directors with executive or operational depth in cybersecurity, which would only provide additional valuable information to investors.

Question 34: A proposed Item 407(j) does not include a definition of the term "expertise" in the context of cybersecurity? Should Item 407(j) define the term "expertise"? If so, how should we define the term?

DDN Answer 34: No, we believe the suggestions made are sufficient as they are focused on applied cyber experience criteria and formally acquired knowledge through structured learning, and/or applied learning in the context of being a cybersecurity practitioner. See DDN Answer 29.

Question 35: Should certain categories of registrants, such as smaller reporting companies, emerging growth companies, or FPI's be excluded from the proposed Item 407(j) disclosure requirement? How would any exclusion affect the ability of investors to assess the cybersecurity risk of a registrant or compare such risk among registrants?

DDN Answer 35: Absolutely no exclusions should be made because of the growth of systemic risk. Smaller issuers present a unique systemic challenge to larger companies as attackers can exploit their lesser developed cybersecurity management practices to target larger companies. A strong system of cybersecurity for America's public companies requires that they all adopt the most basic cybersecurity policies and practices, which Item 407(j) represents. Exclusions will introduce specific weaknesses that can be targeted and exploited, which will create greater risk for the excluded along with the larger issuers through this systemic attack vector. Leaving a weak point in the highly connected nature of the American business ecosystem invites targeted escalation. Item 407(j) must cover every issuer, otherwise, its effectiveness as a key cybersecurity control is defeated for all issuers. Each issuer is only as strong as the weakest link in their connected ecosystem, the proposal needs to cover all issuers for this reason.

Question 36: Should we adopt the proposed Item 407(j)(2) safe harbor to clarify that a director identified as having expertise in cybersecurity would not have any increased level of liability under the federal securities laws as a result of such identification. Are there alternatives we should consider?

DDN Answer 36: Yes, this should be adopted to explicitly address the director liability concern of cyber experts taking these roles, as many of them will be first-time directors. It will reassure them

Bob Zukis
Chief Executive Officer
310.528.9945
ceo@digitaldirectors.network

to attract as large of a candidate pool as possible and alleviate any concerns here while also alerting all corporate directors to their shared responsibility and accountability to this issue.

Question 37: As proposed, disclosure under Item 407(j) would be required in a proxy or information statement. Should we require the disclosure under Item 407(J) to appear in a registrant's proxy or information statement regardless of whether the registrant is relying on General Instruction G(3)? Is this information relevant to a security holder's decision to vote for a particular director?

DDN Answer 37: Yes, it is very relevant to individual director votes for an investor, particularly institutional investors. Cyber risk is a risk with business continuity implications that have material financial and equity risk implications not just to the organization, but to connected ecosystem partners given the growing threat of systemic risk. As such, directors who are cyber experts should be explicitly identified in the proxy or information statement.

In summary, we reiterate our strong support for the broader proposal, especially Item E, and are pleased to provide our comments. We've already been working to advance this issue over the last five years and our support and comments come from our depth of experience and informed insights on this issue. We are America's leader in digital and cyber risk governance, and your proposal has the strong support of the more than 700 technology and cyber leaders who are our members.

America's investors, consumers, and stakeholders expect and deserve the companies they do business with to have cyber competent boardrooms highly capable of governing these complex issues. In hindsight, this proposed rule once passed into law, will be looked upon as a turning point and common-sense regulation that materially advanced America's national security and the competitiveness of American business.

Thank you for your attention and please contact me if you would like to discuss these views.

Sincerely,

Bob Zukis
CEO, Digital Directors Network